REMARKS

The Office rejects claims 1-47 in the subject application. Applicant amends claims 26, 27, 37, and 38. Claims 1-47 (4 independent claims; 47 total claims) remain pending in the application.

Support for the various amendments may be found in the originally filed specification, claims, and figures. No new matter has been introduced by these amendments. Reconsideration of this application is respectfully requested.

35 U.S.C. §102 REJECTION

The Examiner rejects claims 1-47 under 35 U.S.C. §102(e) as allegedly being anticipated by Ishibashi (U.S. Patent No. 6,728,379, issued April 27, 2004, assignee is Sony Corporation). Applicant respectfully traverses the rejection.

Ishibashi discloses a content distribution system using an information processor 100, a content provider 10, a network service provider 20, and a key distribution center 30.[1] A key generator 14 in content provider 10 generates a content encryption key Kce and a content decryption key Kcd. A content encryption section 13 uses content encryption key Kce to encrypt content data stored in a content storage medium 11. A content key encryption section 16 uses a distribution encryption key Kde (received from key distribution center 30) to encrypt content decryption key Kcd and send an encrypted content decryption key Kde (Kcd) to communication section 15. Communication section 15 transmits encrypted content data Kce (Cont) and encrypted content decryption key Kde (Kcd) to communication section 23 of network service provider 20.[2]

Information processor 100 (located at the user) receives encrypted content Kce(Cont) and content decryption key Kde (Kcd) from network service provider 20 (which are then stored in the HDD 110). A communication section 102 receives distribution decryption key Kdd from key distribution center 30 (which is then stored in the memory 134). A controller 120 reads each content data corresponding to a content data selected by the user and sends the selected content data to a cryptography processor 130. A content key decryption section 131 obtains distribution decryption key Kdd from a memory 134 and decrypts encrypted content decryption key Kde (Kcd) corresponding to the content data selected by the user (thereby obtaining content

[1] Ishibashi, Figures 1 and 8.

BEST AVAILABLE COPY

decryption key Kcd). Content decryption key Kcd from content key decryption section 131 is sent to a content decryption section 136, copy controller 137, and content key decryption section 133 in order to be used as shown in Figure 8.[3]

For example, content decryption section 136 uses content decryption key Kcd to decrypt encrypted content Kce (Cont), so that the content data (such as an audio signal) can be converted to an acoustic signal for listening via speaker 104.[4]

<u>Claims 1 and 14: a [first] contents key generation section for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation</u>

The Examiner alleges that the [first] contents key generation section as recited in claims 1 and 14 is taught by key generation section 14 of content provider 10 of Ishibashi. **Ishibashi merely discloses that key generation section 14 generates content encryption key Kce and content decryption key Kcd,[5] but how these keys are generated by key generation section 14 is not disclosed in Ishibashi.**

The Examiner further alleges that "generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation" is taught in column 6 (lines 1-20) of Ishibashi. In such portion, Ishibashi discloses the inhibition of data copy by SCMS (serial copy management system), which only allows one further generation of a data copy through the use of copy control code. In particular, Ishibashi discloses that when a purchased content data is digitally copied at the user-side information processor 100, a copy control code is added to the decrypted content decryption key Kcd and the copy control code is rewritten to a state that the content data may not be copied. **But Ishibashi fails to teach or suggest "generating the contents key <u>based on a second decryption limitation obtained by updating a first decryption limitation</u>" as recited in claims 1 and 14 (and claims 2-13 and 15-25, which variously depend from claims 1 and 14).**

Furthermore, such change in the copy control code in Ishibashi is only performed in the user-side information processor 100 via copy controller 137, but <u>no</u> such alleged change in the copy control code is performed in key generation section 14 of content provider 10.[6] **As such, key generation section 14 of content provider 10 in Ishibashi fails to disclose the [first] contents**

[2] Ishibashi, column 8, line 35 to column 9, line 10.
[3] Ishibashi, column 9, line 53 to column 10, line 52 and Figure 8.
[4] Ishibashi, column 9, linc 53 to column 10, line 8 and Figure 8
[5] Ishibashi, column 8, lines 44-45.
[6] Ishibashi, column 10, lines 55-66.

PAGE 19/21 * RCVD AT 5/18/2006 6:57:56 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/0 * DNIS:2738300 * CSID:602 382 6070 * DURATION (mm-ss):07-14

BEST AVAILABLE COPY

key generation section as recited in claims 1 and 14 (and claims 2-13 and 15-25, which variously depend from claims 1 and 14).

Still further, no contents key is generated based on the portion of Ishibashi cited by the Examiner (i.e., column. 6, lines 1-20). In particular, in such portion (and column 10, line 55 to column 11, line 16), Ishibashi merely describes that content key encryption section 133 encrypts the copy control code and the content decryption key Kcd by a session key Ksession and sends the encrypted content decryption key Ksession (Kcd^{cx}) to communication section 105. As such, Ishibashi fails to disclose the generation of a content encryption key Kce and a content decryption key Kcd (the alleged content keys) in column 6 (line 1-20) of Ishibashi. Rather, this portion of Ishibashi only encrypts already existing content decryption key Kcd.

Claim 1: the decryption device includes a second contents key generation section for generating the contents key from the second decryption limitation

The Examiner alleges that a second contents key generation section is taught by content key decryption section 131 in Ishibashi (which allegedly generates content decryption key Kcd). Content key decryption section 131 merely decrypts the encrypted content decryption key Kde (Kcd) by the distribution decryption key Kdd, so as to output the content decryption key Kcd.[7] As such, such decryption of the encrypted content decryption key Kde (Kcd) is based on the distribution decryption key Kdd, which was generated by key distribution center 30.

Although the Examiner alleges that such generation of the contents key from the second decryption limitation is taught by the copy control code being updated in Ishibashi, such "update" of the copy control code is performed after content key decryption section 131 (by copy controller 137).

Thus, Ishibashi fails to teach or suggest "the decryption device includes a second contents key generation section for generating the contents key from the second decryption limitation" as recited in claim 1 (emphasis added).

[7] Ishibashi, column 10, linc 42-44.

BEST AVAILABLE COPY

Claims 26 and 37

First, per the foregoing discussion of claims 1 and 14, Ishibashi also fails to teach or suggest "a contents key generation section for generating the contents key from the second decryption limitation" as recited in claims 26 and 37 (and claims 27-36 and 38-47, which variously depend from claims 26 and 37).

Second, the Examiner alleges that Ishibashi discloses second information processor 200 is a decryption device, user-side information processor 100 is for performing cryptographic communication in association with an encryption device, and content key decryption section 231 is a contents key generation section for generating the contents key from the second decryption limitation. **But, second information processor 200 fails to disclose "a decryption limitation updating section for updating a first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule" as recited in amended claims 26 and 37.**

CONCLUSION

Thus, the Applicant respectfully submits that the present application is in condition for allowance. Reconsideration of the application is thus requested. Applicant invites the Office to telephone the undersigned if he or she has any questions whatsoever regarding this Response or the present application in general.

Respectfully submitted,

Date: 5-18-06

By: S. Sh
Shahpar Shahpar
Reg. No. 45,875

SNELL & WILMER L.L.P.
400 East Van Buren
Phoenix, Arizona 85004-2202
Phone: (602) 382-6306
Fax: (602) 382-6070
Email: sshahpar@swlaw.com

BEST AVAILABLE COPY